

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A
Property to Be Searched

220 North 34th Street, Milwaukee, Wisconsin to include the storage unit and 2017 Tan Chevrolet Impala, bearing WI license plate AFB4186 used by Trenell HENNING. This address is utilized by Trenell HENNING. Described as a single family, multi-story residence with brown siding and brown trim, there is a brown fence surrounding the backyard of the property and the numbers “220” appear on a front porch column in black lettering. The structure additionally has a rear porch and a brown roof.

ATTACHMENT B
Particular Things to be Seized

1. All records relating to crimes of distribution of a controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances, possession of a machinegun, false statement to a licensed firearms dealer, firearms trafficking, violations of Title 18, United States Code Sections 920(o), 922(a)(6), 924(a)(2), and 933(a)(1) and Title 21, United States Code, Sections 841 and 846, involving Jaiden HENNING and Trenell HENNING between the dates of January 20, 2022, and present date, including:

- A. Records and information relating to a conspiracy to purchase/sell and acquire machine guns;
- B. Records and information relating to the e-mail and social media accounts connected to Jaiden HENNING and Trenell HENNING;
- C. Records and information relating to the identity or location of the suspects;
- D. Records and information relating to communications with Internet Protocol addresses;
- E. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- F. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- G. The contents of all emails associated with the account from January 20, 2022 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- H. The contents of all instant messages associated with the account from January 20, 2022 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with

each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- I. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
 - J. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
 - K. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
 - L. All records pertaining to the types of service used;
 - M. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
 - N. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- A. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- B. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- C. evidence of the lack of such malicious software;
- D. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- E. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- F. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- G. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- H. evidence of the times the COMPUTER was used;
- I. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- J. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- K. records of or information about Internet Protocol addresses used by the COMPUTER;
- L. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- M. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Trenell HENNING to the fingerprint scanner of the device; (2) hold a device found in front of the face of Trenell HENNING and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Case No.23-896M(NJ)

220 North 34th Street, Milwaukee Wisconsin to include the storage
unit and 2017 Tan Chevrolet Impala bearing WI plate AFB-4186
used by Trenell Henning, as further described in Attachment A.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ Eastern _____ District of _____ Wisconsin _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841 & 846	Distribution of a controlled substances; & Conspiracy to distribute and possess
18 U.S.C. §§ 920(o), 922(a)(6),	with the intent to distribute controlled substances. Possession of a machinegun;
924(a)(2), &933(a)(1)	False statement to a licensed firearms dealer, & Firearms trafficking.

The application is based on these facts:

See Attached Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

RICHARD CONNORS

Digitally signed by RICHARD CONNORS
Date: 2023.04.19 14:13:22 -05'00'

Applicant's signature

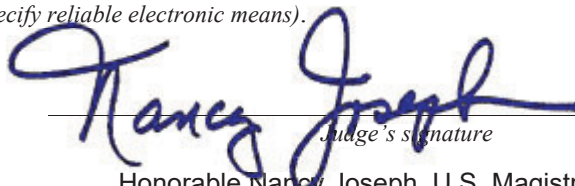
ATF SA Richard Connors

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 4/19/2023

City and state: Milwaukee, Wisconsin



Judge's signature

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Richard Connors, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the TARGET LOCATION, further described in Attachment A, for the things described in Attachment B.

2. I am employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) assigned to the Milwaukee Field Office since October of 2015. I have been employed as a full-time law enforcement officer for approximately seven years. I have received training at the Federal Law Enforcement Training Center in Glynco, GA. I attended the Criminal Investigator Training Program, as well as ATF’s Special Agent Training Program. I have received training in the investigation of unlawful possession of firearms, the unlawful transfer of firearms, and the unlawful dealing in firearms without a dealers’ license. Prior to becoming a Special Agent with the ATF, I received two (2) bachelor’s degrees from Northern Illinois University in the fields of Sociology and International Relations. I have received a master’s degree from Northern Illinois University in the field of American Government.

3. I have received training in the investigation of firearm and drug trafficking. Based on my training, experience, and participation in firearm trafficking investigations, I know and/or have observed the following:

- a. I have utilized informants to investigate firearm and drug trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations distribute these items in Wisconsin and elsewhere;

- b. I have also relied on informants to obtain firearms (as opposed to licensed gun dealers) and controlled substances from individuals on the streets, known as a controlled purchase;
- c. I have experience conducting street surveillance of individuals engaged in firearm and drug trafficking. I have participated in the execution of numerous search warrants where drugs, firearms, ammunition, and magazines have been seized;
- d. I am familiar with the language utilized over the telephone to discuss firearm and drug trafficking, and know that the language is often limited, guarded, and coded;
- e. I know that firearm and drug traffickers often use electronic equipment to conduct these operations; and
- f. I know that firearm and drug traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that firearm and drug traffickers often use nominees to purchase and/or title these assets to avoid scrutiny from law enforcement officials. I also know what firearm and drug traffickers may keep photographs of these items on electronic devices.
- g. It is a common practice for individuals engaged in high level drug and firearm trafficking activities to use multiple locations to conduct their drug and firearm trafficking activities. For example, a “stash house” is a location used to store controlled substances, firearms, and U.S. Currency.
- h. I know large-scale drug and firearms traffickers often purchase and/or title their assets in fictitious names, aliases or the names of relatives, associates or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in the names other than the drug or firearm traffickers, the drug or firearm traffickers actually own and continue to use these assets and exercise dominion and control over them.
- i. I know it is common for persons involved in drug or firearm trafficking and related financial crimes to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and/or expenditure of drug or firearm proceeds, such as ledgers, currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, passbooks, letters of credit, bank drafts, cashier’s checks, bank checks, safe deposit box keys and money wrappers. Because narcotics and firearm trafficking generates large sums of cash, it requires the keeping of detailed records as to the distribution of narcotics and/or firearms as well as the laundering of the proceeds. Such records also typically provide evidence as to the identity of additional criminal associates who are facilitating the laundering of the narcotics proceeds on behalf of the organization. These records, unlike controlled substances or the actual firearms are often maintained for long periods, even several years. These

- items are maintained by the traffickers within residences, stash houses, vehicles, or other locations over which they maintain dominion and control.
- j. I know it is common for drug and firearm traffickers to maintain books, records, receipts, notes ledgers, airline tickets, receipts relating to the purchase of financial instruments and/or the transfer of funds and other papers relating to the transportation, ordering, sale and distribution of controlled substances. That the aforementioned book, records, receipts, notes, ledger, etc., are maintained where the traffickers have immediate access to them.
 - k. It is common practice for individuals who are involved in business activities of any nature to maintain books and records of such business activities for lengthy periods of time. It is also common practice for individuals who maintain these records to keep them in places that are secure but easily accessible such as in their businesses, offices, or personal residence.
 - l. It is also common that individuals who are attempting to conceal their true income from the IRS will maintain records that will establish their true ownership of assets or other expenditures in a secret manner. These records have included bank records, automobile titles, property deeds, cashier's check receipts, money order receipts, wire transfer receipts, documents pertaining to storage facilities or safe deposit boxes, documents or agreements detailing the true ownership of assets, photographs of the true owners with the concealed assets, or other items such as sales receipts, purchase orders, or shipping invoices.
 - m. Likewise, it is common for businesses who engage in transactions with individuals involved in criminal activity to conceal the nature of the transactions through false records such as invoices, by maintaining false financial records, or placing the transaction in a nominee name. These businesses may need to keep these false records for inventory or bookkeeping reasons. However, these false records may be placed in a separate location such as a personal residence, safe, or safe deposit box for concealment.
 - n. I know large-scale drug traffickers often use electronic equipment such as telephones (land-lines and cell phones), pagers, computers, telex machines, facsimile machines, currency counting machines and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug trafficking activities.
 - o. I know when drug or firearms traffickers amass large proceeds from the sale of drugs/firearms, the traffickers attempt to legitimize these profits through money laundering and structuring activities. To accomplish these goals, traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts and otherwise legitimate businesses which generate large quantities of currency.

- p. I know that the Currency Transaction Report (CTR) (Fincen Form 104), which is required to be completed and filed with the IRS by all financial institutions on every currency transaction that exceeds \$10,000, causes tremendous problems with drug and firearm traffickers when they attempt to negotiate their illegal profits at a financial institution; I further know that the courts have recognized that unexplained wealth is probative evidence of crimes motivated by greed, in particular, trafficking in controlled substances.
- q. I know drug and firearm traffickers commonly maintain addresses or telephone numbers in books or papers which reflect names, addresses and/or telephone numbers of their associates in the trafficking organization(s).
- r. I am familiar with computers, cellular telephones, pagers and their uses by drug and firearm traffickers to communicate with suppliers, customers, and fellow traffickers and by those engaged in money laundering and structuring activities to communicate with their associates and financial institutions; That drug and firearm traffickers use these devices to record their transactions and aspects of their lifestyle related to drug dealing, whether in the form of voicemail, email, text messages, video and audio clips, floppy disks, hard disk drives, flash drives, CD's, DVD's, optical disks, Zip disks, flash memory cards, Smart media and any data contained within such computers or cellular telephones, electronic storage media and other settings particular to such devices; I know that such devices automatically record aspects of such communications, such as lists of calls and communications, and any particularized identification assigned to those source numbers or email addresses by the owner of the devices.
- s. Specifically, I know the following information can be retrieved to show evidence of use of the computer to further the drug trade and/or related financial crimes; Computer systems and cellular telephones, including but not limited to system components, input devices, output devices, data storage devices, data transmission devices, and network devices and any data contained within such systems; and computer media and any data contained within such media and other material relating to computer systems and the internet including but not limited to, documentation, operating system software, application or access program disks, manuals, books, brochures, or notes; and computer access codes, user names, log files, configuration files, and passwords, screen names, email addresses, IP addresses and cellular / wireless telephones, SIM cards, any removable storage devices for telephones, and any data contained therein, including but not limited to stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data.

4. That based upon my training and experience, I know that the execution of a search warrant related to remotely stored accounts such as Apple and within email accounts maintained by Apple, and Android, such as “iCloud”, bills, bank statements, photographs, videos, and other items or documents which establish the identities of persons in control of the media. I know electronic devices can be preserved for months and contain records from months prior that would assist investigators with the investigation.

5. That based on my training and experience, I know that individuals purchasing and selling firearms routinely keep emails regarding the purchases and/or sales. These individuals also will keep text messages to prospective buyers of the firearms.

6. I know it is common for firearms purchasers to maintain electronic records, receipts, notes, ledgers, receipts relating to the transportation, ordering and purchase of firearms and that such records are typically kept where the purchaser would have ready access to them including Apple and Android accounts.

7. I have participated in multiple firearm and drug trafficking investigations that involved the seizure of computers, cellular phones, cameras, and other digital storage devices, and the subsequent analysis of electronic data stored within these computers, cellular phones, cameras, and other digital storage devices. In many occasions, this electronic data has provided evidence of the crimes being investigated and corroborated information already known or suspected by law enforcement.

8. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

9. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that possible crimes of distribution of a controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances, possession of a machinegun, false statement to a licensed firearms dealer, firearms trafficking, violations of Title 18, United States Code Sections 920(o), 922(a)(6), 924(a)(2), and 933(a)(1) and Title 21, United States Code, Sections 841 and 846, have been committed by Azjuan K. MERIWETHER, Dontrell Q. FRANKLIN, Jaiden HENNING, and Trenell HENNING and other identified and unidentified subjects. Further probable cause to believe that Trenell HENNING is associated with the properties described in Attachment A and both Jaiden HENNING and Trenell HENNING have active arrest warrants involving Eastern District of Wisconsin Case 2023-CR-69. Further, there is probable cause to believe that located at and in the TARGET LOCATION, more fully described are items that constitute evidence of the crimes committed by Trenell HENNING, as described in Attachment B:

- a. **220 North 34th Street, Milwaukee, Wisconsin** to include the storage unit and 2017 Tan Chevrolet Imapala, bearing WI license plate AFB4186 used by Trenell HENNING. This address is utilized by Trenell HENNING. Described as a single family, multi-story residence with brown siding and brown trim, there is a brown fence surrounding the backyard of the property and the numbers “220” appear on a front porch column in black lettering. The structure additionally has a rear porch and a brown roof.

PROBABLE CAUSE

A. Background

10. Beginning in July 2022, Drug Enforcement Agency (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Waukesha Metro Drug Unit, hereinafter referred to as “case agents,” began investigating an armed drug trafficking organization (ADTO) operating in the Eastern District of Wisconsin (WI) which involves Azjuan K. MERIWETHER, Dontrell Q. FRANKLIN, Jaiden HENNING and Trenell HENNING, and other identified and unidentified

subjects. Through confidential sources, undercover controlled buys, physical surveillance, electronic surveillance, and record jail calls case agents learned the ADTO sells fentanyl, purported to be heroin, methamphetamines, cocaine, ghost guns, and switches.

11. Since July 5, 2022, a confidential source (CS) and an undercover agent (UC) participated in about 18 controlled buys with members of the ADTO including Azjuan K. MERIWETHER, Dontrell Q. FRANKLIN, Savanna J. WILLIAMS, Daniel RODRIGUEZ-PEREZ, Jaiden A. HENNING and Laron N. KING. Between July 2022 and March 2023, CS and/or the UC obtained approximately 750 grams of heroin, which also field tested positive for fentanyl; 240 grams of methamphetamine; and 155 grams of cocaine from the ADTO. Additionally, UC obtained approximately 20 firearms from the ADTO. Some of the firearms were installed with a Glock auto-sear device (switch), which converts a semi-automatic firearm into a full-automatic firearm, and other times the UC just purchased a Glock auto-sear device. The UC obtained approximately nine Glock auto-sear devices from the ADTO. ATF tested fired the Glock auto-sear devices and determined they converted a semi-automatic firearm into a fully automatic firearm, meaning one pull of a firearm trigger caused the firearm to fire multiple bullets.

12. The CS information is credible and reliable, CS has given information concerning individuals involved in illegal activities which has been independently verified through this investigation. The information has been verified through controlled buys, video recordings obtained during the controlled buys, queries through law enforcement databases, and surveillance. CS is cooperating with law enforcement for consideration on pending criminal drug charges in Waukesha County as well as previous drug charges in Kenosha County. CS has no arrests or convictions relating to dishonesty but has had past arrests or convictions for felony drug offenses and other felony bodily harm offenses.

B. Identification of Jaiden HENNING and Trenell HENNING

13. As part of the investigation into the ADTO, case agents attempted to identify the firearms and Glock auto-sear devices sources for the ADTO. During the undercover controlled buy on October 19, 2022, with MERIWETHER, case agents were aware MERIWETHER communicated with one of his firearm sources using Instagram. Case agents obtained a federal search warrant for MERIWETHER's Instagram account and located several firearms contacts with an individual later identified as Jaiden A. HENNING. Case agents later obtained a federal search warrant for Jaiden HENNING's Instagram account also.

14. Between August 7, 2022, and October 29, 2022, MERIWETHER's Instagram account thereal_chefdon92 and ion.wanna.kickit, identified as Jaiden A. HENNING's account, communicated about "switches", which are also known as Glock auto-sear devices. These devices are subject to the rules and regulations of the National Firearms Act (NFA). During MERIWETHER's and Jaiden HENNING's conversations, they routinely refer to Glock auto-sear devices as "buttons."

15. Jaiden HENNING's publicly viewable profile had photos of Jaiden HENNING with gun cases and firearms. Figures 1, 2, 3, 4, 5, and 6 were posted on September 7, 2022. The photos appear to be behind **3506 North 50th Street (lower), Milwaukee, Wisconsin**, which was identified as Jaiden HENNING's residence during the course of this investigation based on information provided by Jaiden HENNING. Figures 5 and 6 depict a black male holding what appears to be a Glock handgun and five separate Glock handgun firearm boxes.



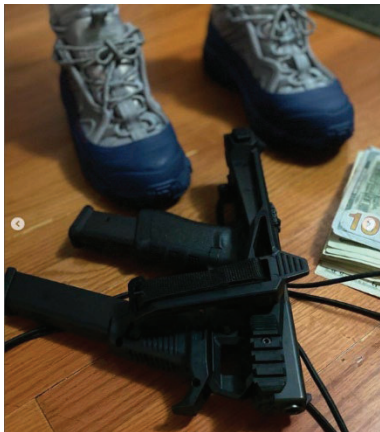
(Figure 1)



(Figure 2)



(Figure 3)



(Figure 4)



(Figure 5)



(Figure 6)

a. **September 12, 2022 Undercover Transaction with MERIWETHER, FRANKLIN, and HENNING**

16. On September 11, 2022, MERIWETHER and HENNING discussed on Instagram the purchase of a Glock auto-sear device (button or switch). They negotiated a price and MERIWETHER asked, “If it’s the metal one.” Jaiden HENNING replied “350 n it’s metal.” Case agents are aware individuals are willing to pay top price for the metal conversion devices as the metal conversion devices hold up to the wear and tear of firearms compared to 3D printed plastic

conversion devices. On September 12, 2022 (date of undercover purchase operation), MERIWETHER began communicating with HENNING via Instagram messenger to arrange the transaction for the Glock auto-sear device. Review of the messages indicated MERIWETHER arrived at Jaiden HENNING's residence (**3506 North 50th Street (lower), Milwaukee, Wisconsin**) to obtain the Glock auto-sear device from Jaiden HENNING at approximately 8:22 A.M. That same day, at approximately 8:42 A.M., MERIWETHER stated, "Even if u got more shit today and tomorrow lmk (let me know) cause he gone be in town today." The UC told MERIWETHER that she/he would be in town that day. Based on my training and experience, MERIWETHER's statements were consistent with him wanting to purchase additional of Glock auto-sear devices or firearms with Jaiden HENNING to resell to the UC.

17. Approximately three hours later on September 12, 2022, the UC purchased a metal Glock auto-sear device from MERIWETHER. The undercover buy took place at 3907 North 24th Street, Milwaukee, Wisconsin. During the transaction, MERIWETHER entered the UC's undercover vehicle and completed a sale of four (4) firearms and a Glock auto-sear switch with the UC. The UC purchased the following firearms and a Glock switch during the transaction in exchange for \$4,000:

- i. NAK9 (Draco), 9 MM, Century Arms with a drum magazine, with serial number RON216548;
- ii. RF-15, multi caliber, Radical Firearms, LLC with serial number 21-105263;
- iii. PT111 Millennium G2, 9 mm, Taurus with serial number TKM53277 with an extended magazine; and
- iv. Bodyguard, 38 special, Smith & Wesson with serial number CPX2831.

18. During the same transaction, MERIWETHER completed the sale of 25.9 grams of heroin to CS in exchange for \$1,250. MERIWETHER was observed by CS to possess "half a

brick” of heroin during the transaction.

19. During this transaction MERIWETHER and UC discussed whether the firearms being sold were previously used in other criminal offenses. MERIWETHER stated that the only firearm he knew to be “legal” was the AR-style rifle he had just sold. UC asked if any of the firearms were “valid,” which based on my training and experience meant not stolen or used in a shooting. MERIWETHER replied, “The only one I don’t know about is the revolver.. the two handguns. But I know both the chops (which based on my training and experience was slang for the AK-style and AR-style firearms) is good. I got the handgun, I got the handgun from the same dude I got the nine, the Draco-nine from. So it might be good as well, but you just never know with handguns.”

b. October 5, 2022 Controlled Transaction with MERIWETHER

20. On October 5, 2022, UC purchased two firearms from MERIWETHER near 23rd Street and Melvina Street, Milwaukee, Wisconsin. The firearms were a 40 Caliber Glock, model 22, bearing serial number BVK7876 with Glock auto-sear device attached, with 14 rounds of ammunition; and a Multi Caliber Franklin Armory, model pistol, bearing serial P-17412 with 10 rounds of ammunition. Case agents review of the Instagram messaging thread between MERIWETHER and Jaiden HENNING indicated MERIWETHER had obtained these firearms from HENNING around September 29, 2022.

21. On September 21, 2022, MERIWETHER messaged Jaiden HENNING: “Wat u got around.” Jaiden HENNING responded: “Shit rn (right now) it’s dry ima lyk (let you know).” On September 25, 2022, Jaiden HENNING messaged MERIWETHER: “U still tryna gram sum?” MERIWETHER responded: “Yeah imma be back Tuesday.” Jaiden HENNING then stated: “Fs

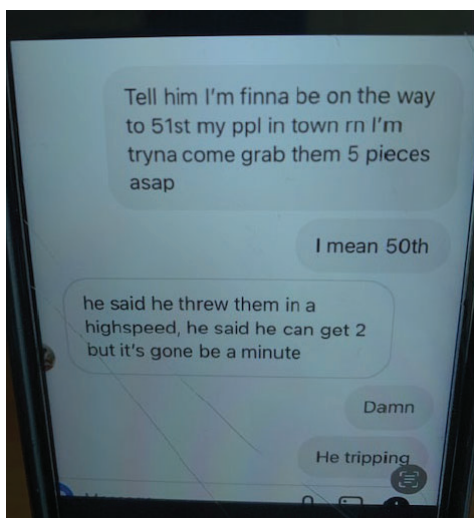
(for sure) Iaa have sum,” and also sent MERIWETHER a photograph of an AR-Pistol that matched the one later purchased by the UC.

22. On September 27, 2022, Jaiden HENNING and MERIWETHER discussed the Glock firearm’s binary trigger and “button” (Glock auto-sear device). Jaiden HENNING and MERIWETHER then discussed prices and eventually agreed to meet and sell the firearms. MERIWETHER did not have enough cash but offered to provide Jaiden HENNING with “grits” of “b” or “g.” Based on my training, experience, and this investigation, I am aware “grit” is a term used for grams by individuals involved with drug trafficking. I am also aware that “b” and “g” are used to describe “boy” or “girl” and that “boy” is a term used for cocaine and “girl” is a term used for heroin. When MERIWETHER was on his way to Jaiden HENNING’s residence MERIWETHER requested Jaiden HENNING bring a “scat.” Based on my training and experience, “scat” is a term used by individuals involved with drug trafficking for scale. Further, based on my training and experience, the messages between MERIWETHER and Jaiden HENNING were consistent with Jaiden HENNING trading a firearm with MERIWETHER for controlled substances.

c. October 19, 2022 Undercover Transaction with MERIWETHER and FRANKLIN

23. On October 14, 2022, Jaiden HENNING sent MERIWETHER several Instagram messages, explaining that Jaiden HENNING obtained five Glock auto-sear devices that were available to be purchased by MERIWETHER. Jaiden HENNING informed MERIWETHER the price for each Glock auto-sear device would be \$400. On this same date, approximately 19 minutes after Jaiden HENNING messaged MERIWETHER, MERIWETHER contacted the UC about purchasing switches, citing that MERIWETHER’s source had just obtained multiple switches. On

October 19, 2022, Jaiden HENNING messaged MERIWETHER “Call me asap.” Jaiden HENNING and MERIWETHER chat and later Jaiden HENNING sent MERIWETHER a message indicating Jaiden HENNING no longer had the switches (Figure 7). MERIWETHER later showed the UC this message to explain why MERIWETHER did not have the Glock auto-sear devices during a controlled buy on October 19, 2022.



(Figure 7)

d. November 16, 2022 Undercover Transaction with MERIWETHER and Jaiden HENNING

24. On September 12, 2022, Jaiden HENNING, messaged MERIWETHER “I can build them mfs for \$400 tho, I got the parts alr I just gotta go grab a lower, I got the upper ready.” Based on case agents training and experience, Jaiden HENNING’s statements were consistent with Jaiden HENNING discussing the manufacturing of an AR-15 style firearm. The “lower” part of an AR-15 style platform is classified as the firearm and can be purchased from a federal firearms licensed dealer (FFL). The “upper” can be purchased online and wherever people sell gun parts. Assembling a lower and upper complete an AR-15 style platform rifle. Based on training and experience, case agents are aware people who are able to legal purchase firearms, will buy the

lower from an FFL. The remaining parts will then be purchased separately to assemble a fully functioning rifle.

25. On November 16, 2022, MERIWETHER met CS and the UC at North 55th Street and West Keefe Avenue, Milwaukee, Wisconsin. MERIWETHER approached the UC's vehicle and entered via the rear driver's side door. MERIWETHER had a large black duffle style bag with him and completed the transactions with the UC and CS. MERIWETHER provided 27.6 grams of heroin, which later field tested positive for fentanyl, to CS. CS provided MERIWETHER with \$5,000 to cover the purchase of the 27.6 grams of heroin and as a buy in to a "brick of heroin." MERIWETHER provided the UC with a firearm, later identified as an AM-15, Anderson Manufacturing Pistol with serial number 22019470, with 26 rounds of ammunition. The UC provided \$1500 to MERIWETHER in exchange for the AM-15.

26. After this controlled buy, case agents conducted surveillance and followed MERIWETHER to the address of **3506 North 55th Street (lower), Milwaukee, Wisconsin**, Jaiden HENNING's residence. Case agents observed Jaiden HENNING exit MERIWETHER's vehicle and walk to the side door of the duplex at **3506 North 55th Street (lower), Milwaukee, Wisconsin**.

27. Case agents determined the AM-15, Anderson Manufacturing Pistol with serial number 22019470, was actually a lower part of an AR-15 style platform that was later connected to an upper receiver, as described previously. The firearm purchased from MERIWETHER was originally purchased by Trenell HENNING, who has been identified as Jaiden HENNING's father, just six days prior to the undercover transaction.

28. Case agents obtained ATF Form 4473 from Fleet Farm located at N96 W18200 County Line Road, Germantown, Wisconsin detailing the purchase of one Anderson

Manufacturing receiver, model AM-15, bearing serial number 22019470. On November 4, 2022, Trenell HENNING completed the paperwork for the firearm. Initially, HENNING was delayed by the FBI NICS system. Trenell HENNING then obtained the firearm from Fleet Farm on November 10, 2022. On the Fleet Farm Firearms order form, Trenell HENNING listed his address on ATF Form 4473 as **3143 North 55th Street, Milwaukee, Wisconsin**. Under question 11a which stated “Are you the actual transferee/buyer of the firearm(s) listed?” Trenell HENNING marked “yes.” Six days later this firearm was sold to UC by Meriwether with Jaiden HENNING in MERIWETHER’s vehicle.

C. Cell Phone Used

a. 414-573-3875 (Trenell HENNING)

29. On November 4, 2022, Trenell HENNING filled out ATF Form 4473 at the Fleet Farm located in Germantown, WI and provided his telephone number 414-573-3875.

30. Case agents reviewed record from the Milwaukee Police Department, which indicated that April 13, 2022, officers were dispatched to 220 N. 34th Street, Milwaukee, Wisconsin, for a domestic violence related issue. The caller stated her boyfriend at the time, Trenell HENNING, pushed her, and grabbed her by the throat in an effort to prevent her from leaving. The caller provided a phone number for Trenell HENNING as 414-573-3875.

31. Case agents have also reviewed call detail records for Jaiden HENNING’s telephone 414-218-3435. Investigators received those results on or about January 6, 2023. Between September 1, 2022, and December 27, 2022, Jaiden HENNING’s telephone 414-218-3435 contacted Trenell HENNING’s telephone 414-573-3875 a total of 264 occasions. Your affiant further believes this to be Jaiden HENNING’s number due to the frequent contacts with his father.

32. Case agents also reviewed law enforcement database, which indicated Trenell HENNING is listed to telephone 414-573-3875.

33. Finally, on April 13, 2023, a case agents obtained records from 414-573-3875 carrier, AT&T, which indicated Trenell HENNING as the listed user.

b. 414-218-3435 (Jaiden HENNING)

34. During the investigation case agents identified Jaiden HENNING's telephone as 414-218-3435 . Case agents identified this number after reviewing Jaiden HENNING's Instagram account. Instagram records provided the verified account phone number for Jaiden HENNING's account as 414-218-3435. Further, during the course of the conversations in the Instagram return, Jaiden HENNING provided 414-218-3435 to multiple individuals. Between the dates of January 6, 2022, and January 13, 2023, Jaiden HENNING provided the above number to individuals on 9 separate occasions. One such occasion was to arrange a firearm purchase with a co-conspirator of the investigation who has also been federally indicted. This conversation occurred on September 28, 2022.

35. Case agents reviewed call details records between Jaiden HENNING's telephone 414-218-3435 and MERIWETHER's telephone 414-999-6172, which was used to arrange numerous controlled buys. Between February 19, 2022, and MERIWETHER's arrest on December 27, 2023, Jaiden HENNING's telephone 414-218-3435 and MERIWETHER were in contact 19 times. Those contacts included three calls between Meriwether and Jaiden HENNING prior to the October 5, 2022, controlled buy; two calls prior to November 15, 2022; and four calls on November 16, 2022, the day of the controlled buy.

36. Further, on October 26, 2022, Jaiden HENNING was stopped by the Germantown Police Department during that traffic stop. During that matter, a juvenile male seated in the rear

seat of Jaiden HENNING's vehicle, was observed stealing a firearm magazine from Fleet Farm in Germantown, WI. Officers found probable cause to search the vehicle and located a backpack containing suspected marijuana. Jaiden HENNING provided his phone number to officers that date at 414-218-3435.

37. Case agents also reviewed law enforcement database, which indicated Jaiden HENNING as the subscriber for 414-218-3435.

38. Finally, on April 13, 2023, a case agents obtained records from 414-218-3435 carrier, AT&T, which indicated Jaiden HENNING as the listed user.

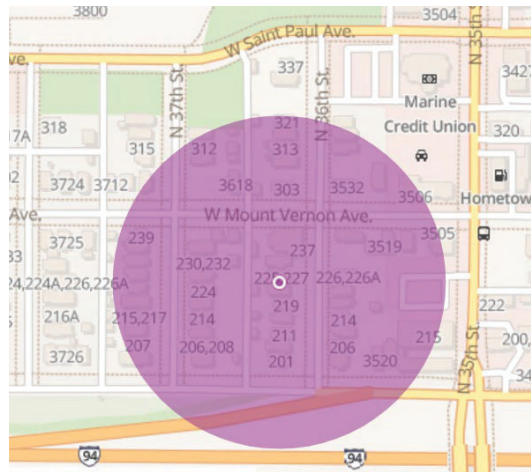
D. Indictment

39. On April 11, 2023, a federal grand jury in the Eastern District of Wisconsin returned a thirty-one-count indictment against MERIWETHER, Jaiden HENNING, Trenell HENNING and other members of the ADTO. Trenell HENNING was indicted for one count of knowingly making a false statement to a licensed firearms dealer, in violation of Title 18, United States Code Sections 922 (a)(6) and 924(a)(2). Additionally, Jaiden HENNING was indicted on one count of conspiracy to possess with intent to distribute and distribute a controlled substance, in violation of Title 21, United States Code Sections 841 and 846; one count of possession of a machinegun, in violation of Title 18, United States Code Section 922(o); one count of distribution of a controlled substance, in violation of Title 21, United States Code Section 841; and firearms trafficking, in violation of Title 18, United States Code Sections 933(a)(1) and 2(a). On April 12, 2023, arrest warrants were issued for Trenell HENNING and Jaiden HENNING and are currently active.

E. TARGET LOCATION

a. 220 North 34th Street, Milwaukee, Wisconsin, Milwaukee, Wisconsin

40. On April 14, 2023, the Magistrate Judge Nancy Joseph authorized a cell phone ping warrant for information associated with Trenell HENNING's telephone 414-573-3875. The warrant was served on the service provider AT&T. The first ping for Trenell HENNING's telephone 414-573-3875 was provided at approximately 3:02AM on April 15, 2023. The ping placed Trenell HENNING near the residence of **220 North 34th Street, Milwaukee, Wisconsin**. I am aware **220 North 34th Street, Milwaukee, Wisconsin** is the address of a longtime girlfriend of Trenell HENNING's identified as Rebecca Lagoo. Rebecca Lagoo had reported to police in the past, (June 24, 2018 and April 13, 2022) that Trenell HENNING had battered her. The April 13, 2022 altercation took place at **220 North 34th Street, Milwaukee, Wisconsin**. The first ping is provided below in Figure 8.



(Figure 8)

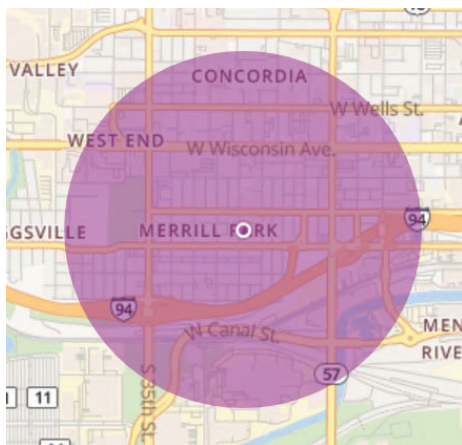
41. Since the pings began being provided to case agents, Trenell HENNING's telephone 414-573-3875 has spent each night at or near **220 North 34th Street, Milwaukee, Wisconsin**.

42. On April 16, 2023, case agents traveled to **220 North 34th Street, Milwaukee, Wisconsin**, to conduct physical surveillance. Parked on the rear parking slab of **220 North 34th Street, Milwaukee, Wisconsin** was a 2017 Tan Chevrolet Impala, bearing WI license plate AFB4186. Your affiant is aware

this license plate is registered to Trenell HENNING at the location of 3143 North 55th Street, Milwaukee, WI.

43. On April 17, 2023, surveillance units once again set up on **220 North 34th Street, Milwaukee, Wisconsin**. At approximately 10:00 am, case agents observed a black male, whom they recognized was Trenell HENNING, and an unknown white female exit the only gate which provides access to the yard directly behind **220 North 34th Street, Milwaukee, Wisconsin**. HENNING was wearing a neon yellow, construction style safety jacket. HENNING and the unknown female got into Trenell HENNING's Chevrolet Impala, with HENNING taking the driver's seat. The vehicle was parked in the east alley directly behind **220 North 34th Street, Milwaukee, Wisconsin**. A short time later the vehicle traveled southbound through the alley and drove out of the area.

44. I am aware on the early morning hours of April 19, 2023, Trenell HENNING was once more pinging at **220 North 34th Street, Milwaukee, Wisconsin**. The current ping for Trenell HENNING places his cell phone in the area of **220 North 34th Street, Milwaukee, Wisconsin**, as of 1:00 PM (April 19, 2021) (Figure 9). I am aware that surveillance units observed Trenell HENNING's Chevrolet Impala registered parked in the rear of **220 North 34th Street, Milwaukee, Wisconsin** on April 19, 2023. For the reasons stated above, your affiant believes Trenell HENNING to be staying at **220 North 34th Street, Milwaukee, Wisconsin**.



(Figure 9)

TECHINICAL BACKGROUND

45. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **TARGET LOCATION**, in whatever form they are found. One form in which the records might be found is data stored on a cellular telephone or computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

46. *Probable cause.* I submit that if a computer, cellular telephone, or electronic storage medium is found at the **TARGET LOCATION**, there is probable cause to believe records associated with Trenell HENNING's and Jaiden HENNING's activities will be stored on the same, for at least the following reasons:

- Based on my knowledge, training, and experience, I know that Trenell HENNING and Jaiden HENNING uses cellular telephones and Jaiden HENNING uses social media applications to communicate.
- I also know, based on my knowledge, training, and experience, that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this

evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

47. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how such electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET LOCATION** because:

- Data on the computer, cellular telephone, or storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- As explained herein, information stored within a computer, cellular telephone, and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatory or exculpatory the computer owner. Further, computer and storage media

activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- A person with appropriate familiarity with how a cellular telephone or computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a cellular telephone or computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- Further, in finding evidence of how a cellular telephone or computer was used, the purpose of its use, who used it, and when, sometimes it is necessary

to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

- I know that when an individual uses a cellular telephone or computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The cellular telephone or computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The cellular telephone or computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a cellular telephone or computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

48. *Necessity of seizing or copying entire computers, cellular telephones, or storage media.*

In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of cellular telephone or computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following: (i) The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be

impractical and invasive to attempt on-site; (ii) Technical requirements. Cellular telephone and computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge; and (iii) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off- site reviewing with specialized forensic tools.

49. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying cellular telephones, computers, and storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

50. Because multiple people share the **TARGET LOCATION**, it is possible that the **TARGET LOCATION** will contain cellular telephones, computers, or storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

51. *Unlocking Apple brand devices:* I know based on my training and experience, as well as from information found in publicly available materials including those published by Apple, that Apple devices are used by many people in the United States, and that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint

(collectively, “fingerprint”) or facial recognition in lieu of a numeric or alphanumeric passcode or password. These features are called Touch ID and Face ID, respectively. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device’s contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made. If Touch ID enabled Apple devices are found during a search of the **TARGET LOCATION**, the passcode or password that would unlock such the devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of any Apple device(s) found during the search of the **TARGET LOCATION** to the device’s Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant. In my training and experience, the person who is in possession of a device

or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the **TARGET LOCATION** in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Apple device(s) found in the **TARGET LOCATION** as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the **TARGET LOCATION** to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the **TARGET LOCATION** for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

CONCLUSION

52. Based on the forgoing, I believe there is probable cause to believe Jaiden HENNING, Trenell HENNING, and other known and unknown individuals have and are committing violations of distribution of a controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances, possession of a machinegun, false

statement to a licensed firearms dealer, firearms trafficking, violations of Title 18, United States Code Sections 920(o), 922(a)(6), 924(a)(2), and 933(a)(1) and Title 21, United States Code, Sections 841 and 846. I further believe that there is probable to believe that located at and in the **TARGET LOCATION** and/or on Jaiden HENNING and Trenell HENNING, further described in Attachment A, there is evidence of these crimes, all of which is detailed more specifically in Attachment B, that a warrant issue authorizing the search of the same.

ATTACHMENT A
Property to Be Searched

220 North 34th Street, Milwaukee, Wisconsin to include the storage unit and 2017 Tan Chevrolet Impala, bearing WI license plate AFB4186 used by Trenell HENNING. This address is utilized by Trenell HENNING. Described as a single family, multi-story residence with brown siding and brown trim, there is a brown fence surrounding the backyard of the property and the numbers “220” appear on a front porch column in black lettering. The structure additionally has a rear porch and a brown roof.

ATTACHMENT B
Particular Things to be Seized

1. All records relating to crimes of distribution of a controlled substances, conspiracy to distribute and possess with the intent to distribute controlled substances, possession of a machinegun, false statement to a licensed firearms dealer, firearms trafficking, violations of Title 18, United States Code Sections 920(o), 922(a)(6), 924(a)(2), and 933(a)(1) and Title 21, United States Code, Sections 841 and 846, involving Jaiden HENNING and Trenell HENNING between the dates of January 20, 2022, and present date, including:

- A. Records and information relating to a conspiracy to purchase/sell and acquire machine guns;
- B. Records and information relating to the e-mail and social media accounts connected to Jaiden HENNING and Trenell HENNING;
- C. Records and information relating to the identity or location of the suspects;
- D. Records and information relating to communications with Internet Protocol addresses;
- E. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- F. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- G. The contents of all emails associated with the account from January 20, 2022 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- H. The contents of all instant messages associated with the account from January 20, 2022 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with

each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

- I. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
 - J. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
 - K. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
 - L. All records pertaining to the types of service used;
 - M. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
 - N. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- A. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- B. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- C. evidence of the lack of such malicious software;
- D. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- E. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- F. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

- G. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- H. evidence of the times the COMPUTER was used;
- I. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- J. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- K. records of or information about Internet Protocol addresses used by the COMPUTER;
- L. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- M. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Trenell HENNING to the fingerprint scanner of the device; (2) hold a device found in front of the face of Trenell HENNING and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.